a

WHAT IS CLAIMED IS;

~~PATENT CLAIMS~~

Sub A7

~~1.~~ Method for encryption of information for a radio transmission and for authentication of subscribers (S1, S2) in a communication system (UNM), that

- comprises an access network (ACN) having equipment (BS, BSC) for the radio transmission as well as at least one core network (CON1, CON2) having a respective equipment (AC, AC') for the subscriber authentication,
- allocates a radio channel (RCH) for the transmission of the information via a radio interface (AI) from/to at least one base station (BS) of the access network (ACN),

whereby

- public keys (PUK1-MT, PUK-BS) are mutually transmitted between a mobile station (MT) and the base station (BS) via the radio interface (AI),
- the public key (PUK1-MT or, respectively, PUK-BS) received by the base station (BS) or, respectively, mobile station (MT) is employed for encryption of the information to be subsequently transmitted via the radio interface (AI),
- the encrypted information received by the mobile station (MT) or, respectively, base station (BS) are deciphered on the basis of a private key (PRK1-MT, PRK1-BS) that is allocated to the transmitted, public key (PUK1-MT, PUK-BS) in the mobile station (MT) or, respectively, in the base station (BS), and whereby
- a subscriber-specific means (SIN) of the mobile station (MT) implements the authentication of the respective core network (CON1, CON2), and the means (AC, AC') of the core network (CON1, CON2) implements the authentication of the subscriber (S1, S2) on the basis of encrypted information that have been mutually sent.

2. Method according to claim 1, whereby

- a first public key (PUK1-MT) is first sent from the mobile station (MT) to the base station (BS), which employs it for the encryption of the information to be sent by the mobile station (MT);
- a public key (PUK-BS) is sent from the base station (BS) to the mobile station (MT), which employs it for the encryption of the information to be sent to the base station (BS); and, subsequently,
- the mobile station (MT) sends a second public key (PUK2-MT) to the base station (BS).

3. Method according to claim 2, whereby the second public key (PUK2-MT) replaces the first key (PUK1-MT) sent to the base station (BS).

4. Method according to claim 1, whereby

- the base station (BS) first sends a first public key (PUK1-BS) to the mobile station (MT) that employs for encryption of the information to be sent to the base station (BS);
- the mobile station (MT) sends a public key (PUK-MT) to the base station (BS) that employs for the encryption of the information to be sent to the mobile station (MT); and, subsequently,
- the base station (BS) sends a second public key (PUK2-BS) to the mobile station (MT).

5. Method according to claim 4, whereby the second public key (PUK2-BS) replaces the first key (PUK1-BS) sent to the base station (BS).

6. Method according to one of the preceding claims, whereby
- the mobile station (MT) sends a subscriber identity (SID) of the subscriber (S1, S2) and an authentication request (aureq-mt) to the core network (CON1, CON2) in encrypted form, and the means (AC, AC') of the core network (CON1, CON2) returns an authentication reply (aures-co) in encrypted form;
- the mobile station (MT) implements an authentication procedure for checking the identity of the core network (CON1, CON2).

7. Method according to claim 6, whereby
- the means (AC, AC') of the core network (CON1, CON2) sends an authentication request (aureq-co) in addition to the authentication reply (aures-co) in encrypted form, and the mobile station (MT) returns an authentication reply (aures-mt) to the means (AC) in encrypted form;
- the means (AC, AC') implements an authentication procedure for checking the subscriber identity (SID).

8. Method according to one of the preceding claims, whereby secret keys (ki) are employed for the authentication procedure.

9. Method according to one of the preceding claims, whereby the access network (ACN) services at least two core networks (CON1, CON2) in parallel and one or more subscribers (S1, S2) that can use the mobile station (MT) in parallel are registered and authenticated in different core networks (CON1, CON2).

10. Method according to one of the claims 1 through 8, whereby the access network (ACN) services a core network (CON) in which a plurality of subscribers (S1, S2) that can use the mobile station (MT) in parallel are registered and authenticated.

11. Method according to one of the preceding claims, whereby the access network (ACN) an the core network or networks (CON1, CON2) are administered by different network operators.

12. Communication system for encryption of information for a radio transmission and for authentication of subscribers (S1, S2), comprising

- an access network (ACN) having equipment (BS, BSC) for the radio transmission as well as at least one core network (CON1, CON2) having a respective means (AC, AC') for the subscriber authentication,
- a radio channel (RCH) for transmission of the intervention via a radio interface (AI) from/to at least one base station (BS) of the access network (ACN),

and comprising

- memory devices (MSP, BSP) in a mobile station (MT) and in the base station (BS) for storing public keys (PUK1-MT, PUK-BS) and private keys PRK1-BS, PRK1-BS [sic]) that are allocated to the public keys (PUK1-MT, PUK-BS),
- transmission devices (MSE, BSE) in the mobile station (MT) and in the base station (BS) for mutually sending the public keys (PUK1-MT, PUK1-BS) via the radio interface (AI),
- control devices (MST, BST) in the mobile station (MT) and in the base station (BS) for encryption of the information to be subsequently sent via the radio interface (A1) upon employment of the public keys (PUK1-MT or, respectively, PUK-BS) received by the base station (BS) or, respectively, mobile station (MT) and for deciphering the received, encrypted information on the basis of the stored, appertaining private key (PRK1-MT, PRK1-BS),

and comprising

- a subscriber-specific means (SIN) in the mobile station (MT) and a means (AC, AC') in the respective core network (CON1, CON2) for the implementation of the authentication of the core network (CON1, CON2) as well as for the authentication of the subscribers (S1, S2) on the basis of mutually transmitted, encrypted information.

13. Communication system according to claim 12, comprising an access network (ACN) to which at least two core networks (CON1, CON2) are connected in parallel for the registration and authentication of one or more subscribers (S1, S2) that can use the mobile station (MT) in parallel in different core network (CON1, CON2).

14. Communication system according to claim 12, comprising an access network (ACN) to which a core network (CON1) is connected for the registration and authentication of a plurality of subscribers (S1, S2) that can use the mobile station (MT) in parallel.

15. Communication system according to one of the preceding claims, comprising an access network (ACN) and one or more core networks ~~(CON1, CON2) that~~ exhibit different network operators.